

DOCKET NO.: 212810US2PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: UGA Shinsuke et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP00/09128

INTERNATIONAL FILING DATE: December 22, 2000

FOR: RADIO COMMUNICATION APPARATUS AND RADIO COMMUNICATION METHOD

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	11-370657	27 December 1999

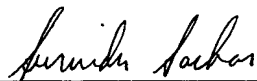
Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP00/09128.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 1/97)


Marvin J. Spivak
Attorney of Record
Registration No. 24,913
Surinder Sachar
Registration No. 34,423

THIS PAGE BLANK (USPTO)

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

22.12.00

JP00/9128

4
別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

1999年12月27日

REC'D 23 FEB 2001

WIPO

PCT

出願番号
Application Number:

平成11年特許願第370657号

出願人
Applicant(s):

三菱電機株式会社

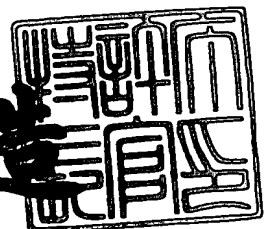
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 2月 9日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3004801

【書類名】 特許願
【整理番号】 522214JP01
【提出日】 平成11年12月27日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/06

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 宇賀 晋介

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 松山 浩司

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 近澤 武

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100099461

【弁理士】

【氏名又は名称】 溝井 章司

【選任した代理人】

【識別番号】 100111497

【弁理士】

【氏名又は名称】 波田 啓子

【選任した代理人】

【識別番号】 100111800

【弁理士】

【氏名又は名称】 竹内 三明

【手数料の表示】

【予納台帳番号】 056177

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9903016

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線通信装置

【特許請求の範囲】

【請求項 1】 データを入力する端末インタフェース部と、
端末インタフェース部が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から出力されたデータを入力して変調し送信する無線通信部と

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部とを備えたことを特徴とする無線通信装置。

【請求項 2】 上記秘匿・完全性保証処理部は、無線通信制御部から制御信号を入力し、入力した制御信号に基づいて端末インタフェース部からデータを選択的に入力するとともに、入力したデータに対して秘匿処理を行い、秘匿処理したデータを無線通信部に出力することを特徴とする請求項 1 記載の無線通信装置。

【請求項 3】 上記端末インタフェース部は、透過データと非透過データとを出力し、

上記無線通信制御部は、非透過データを端末インタフェース部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを端末インタフェース部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする請求項 2 記載の無線通信装置。

【請求項 4】 上記秘匿・完全性保証処理部は、無線通信制御部と平行ルインタフェースで接続されていることを特徴とする請求項 1 記載の無線通信装置。

【請求項 5】 上記秘匿・完全性保証処理部は、端末インタフェース部とシ

リアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする請求項 2 記載の無線通信装置。

【請求項 6】 上記秘匿・完全性保証処理部は、
入力したデータを暗号化する暗号化部を有する秘匿処理部と、
入力したデータに対して完全性認証子を付加する完全性認証子付加部を有する
完全性保証処理部と

を備えたことを特徴とする請求項 1 記載の無線通信装置。

【請求項 7】 上記秘匿処理部は、複数の暗号化部を有することを特徴とする請求項 6 記載の無線通信装置。

【請求項 8】 上記完全性保証処理部は、複数の完全性認証子付加部を有することを特徴とする請求項 6 記載の無線通信装置。

【請求項 9】 上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する 1 つのモジュールであり、その 1 つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行することを特徴とする請求項 6 記載の無線通信装置。

【請求項 10】 データを受信して復調する無線通信部と、
無線通信部により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御部と、
無線通信制御部により処理されたデータを入力して出力する端末インタフェース部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と
を備えたことを特徴とする無線通信装置。

【請求項 11】 上記秘匿・完全性保証処理部は、
無線通信制御部から制御信号を入力し、入力した制御信号に基づいて無線通信部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

秘匿処理したデータを端末インタフェース部に出力することを特徴とする請求項 10 記載の無線通信装置。

【請求項 12】 上記無線通信部は、透過データと非透過データとを出力し

上記無線通信制御部は、非透過データを無線通信部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを無線通信部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする請求項 11 記載の無線通信装置。

【請求項 13】 上記秘匿・完全性保証処理部は、無線通信制御部と平行インタフェースで接続されていることを特徴とする請求項 10 記載の無線通信装置。

【請求項 14】 上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする請求項 11 記載の無線通信装置。

【請求項 15】 上記秘匿・完全性保証処理部は、
入力したデータを復号化する復号化部を有する秘匿処理部と、
入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部を有する完全性保証処理部と
を備えたことを特徴とする請求項 10 記載の無線通信装置。

【請求項 16】 上記秘匿処理部は、複数の復号化部を有することを特徴とする請求項 15 記載の無線通信装置。

【請求項 17】 上記完全性保証処理部は、複数の完全性確認部を有することを特徴とする請求項 15 記載の無線通信装置。

【請求項 18】 上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する 1 つのモジュールであり、その 1 つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部のいずれかの処理を実行することを特徴とする請求項 15 記載の無線通信装置。

【請求項 1 9】 データを無線通信する無線通信装置において、
 データを入出力する端末インタフェース部と、
 プロトコルに基づいてデータの処理をする無線通信制御部と、
 データを無線通信する無線通信部と、
 端末インタフェース部と無線通信制御部と無線通信部との三者間に設けられ、

~~無線通信制御部との間でデータに対して少なくともデータを暗号化復号化する秘~~
 匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端
 末インタフェース部から無線通信部へのデータを暗号化するとともに無線通信部
 から端末インタフェース部へのデータを復号する秘匿・完全性保証処理部と
 を備えたことを特徴とする無線通信装置。

【請求項 2 0】 上記秘匿・完全性保証処理部は、
 入力したデータに対して秘匿処理を行う秘匿処理部と、
 入力したデータに対して完全性保証処理を行う完全性保証処理部と
 を個別に備えたことを特徴とする請求項 1 9 記載の無線通信装置。

【請求項 2 1】 上記秘匿処理部は、
 端末インタフェース部から無線通信部へのデータを暗号化する暗号化部と、
 無線通信部から端末インタフェース部へのデータを復号化する復号化部とを個
 別に有することを特徴とする請求項 1 9 記載の無線通信装置。

【請求項 2 2】 上記完全性保証処理部は、
 入力したデータに対して完全性保証処理を行う完全性認証子を付加する完全性
 認証子付加部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を
 確認する完全性確認部と
 を個別に有することを特徴とする請求項 1 9 記載の無線通信装置。

【請求項 2 3】 上記通信装置は、携帯型移動電話機であることを特徴とす
 る請求項 1 9 記載の無線通信装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、携帯電話機等の無線通信装置に関するものである。特に、データの秘匿処理と完全性保証処理を行う携帯電話機に関するものである。

【0002】

【従来の技術】

図14は、従来の携帯電話機500を示す図である。

従来の携帯電話機500には、端末IF（インタフェース）部510と無線通信制御部520と無線通信部530が備えられている。端末IF部510は、携帯電話機500のユーザとのインタフェースを行う部分である。無線通信制御部520は、携帯電話機500全体の通信制御とプロトコルに基づくデータの変換とデータ処理とを行う部分である。無線通信部530は、データを変調復調し、無線通信可能とする部分である。無線通信部530は、OSI（Open Systems Interconnection）で定義されている7階層のレイヤの内、最下層である物理レイヤ（レイヤ1）をサポートしている部分である。無線通信部530には、秘匿処理部540が設けられている。秘匿処理部540は、無線通信部530で取り扱われる物理レイヤのデータに対して暗号化処理、或いは、復号化処理を行う部分である。秘匿処理部540を設けることによりアンテナ541で送受信されるデータを盗聴しても暗号化されているので、解読されない限りにおいて盗聴者が有意な情報を得ることはできないこととなる。

【0003】

【発明が解決しようとする課題】

従来の携帯電話機500は、秘匿処理部540を無線通信部530の内部に有している。このため、秘匿処理部540が秘匿対象とするデータは、物理レイヤ（レイヤ1）のデータである。物理レイヤでは、そのデータがユーザデータであるか制御データであるかは特定できない。携帯電話機により送受信されるデータの中には、各種ユーザデータ及びシグナリングデータなどいろいろな種類があり、そのデータの種類に応じて秘匿処理を行ったり、或いは、そのデータの重要性に応じてデータの完全性を保証したりする必要がある。従来の構成のように、秘匿処理部540がレイヤ1に設けられていたのでは、レイヤ1においてはデータの種別が区別できないため、データの種別に応じて秘匿処理や完全性の保証をす

るということができなかった。

【0004】

この発明の好適な実施の形態では、データの種類に応じて秘匿処理や完全性保証処理が選択的に行える無線通信装置を得ることを目的とする。

【0005】

また、この発明の好適な実施の形態では、OSIの7つの階層の内、レイヤ2（データリンク層）以上の上位レイヤにおいて秘匿処理と完全性保証処理が行える無線通信装置を得ることを目的とする。

【0006】

また、この発明の好適な実施の形態では、秘匿処理と完全性保証処理との両方又は一方をデータの種類に応じて選択的に行える無線通信装置を得ることを目的とする。

【0007】

また、この発明の好適な実施の形態では、無線通信装置が複数のチャネルを有している場合においてもチャネル毎に秘匿処理と完全性保証処理とが行える無線通信装置を得ることを目的とする。

【0008】

また、この発明の好適な実施の形態では、あるレイヤ、或いは、サブレイヤを透過する透過データと、そのレイヤ、或いは、サブレイヤを透過しない非透過データとを区別して、秘匿処理と完全性保証処理とを選択的に行う無線通信装置を得ることを目的とする。

【0009】

【課題を解決するための手段】

この発明に係る無線通信装置は、データを入力する端末インタフェース部と、端末インタフェース部が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から出力されたデータを入力して変調し送信する無線通信部と

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づい

て、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部とを備えたことを特徴とする。

【0010】

上記秘匿・完全性保証処理部は、無線通信制御部から制御信号を入力し、入力した制御信号に基づいて端末インタフェース部からデータを選択的に入力するとともに、入力したデータに対して秘匿処理を行い、秘匿処理したデータを無線通信部に出力することを特徴とする。

【0011】

上記端末インタフェース部は、透過データと非透過データとを出力し、上記無線通信制御部は、非透過データを端末インタフェース部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを端末インタフェース部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする。

【0012】

上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする。

【0013】

上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする。

【0014】

上記秘匿・完全性保証処理部は、入力したデータを暗号化する暗号化部を有する秘匿処理部と、入力したデータに対して完全性認証子を付加する完全性認証子付加部を有する完全性保証処理部とを備えたことを特徴とする。

【0015】

上記秘匿処理部は、複数の暗号化部を有することを特徴とする。

【0016】

上記完全性保証処理部は、複数の完全性認証子付加部を有することを特徴とする。

【0017】

上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する1つのモジュールであり、その1つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部のいずれかの処理を実行することを特徴とする。

【0018】

この発明に係る無線通信装置は、データを受信して復調する無線通信部と、無線通信部により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部により処理されたデータを入力して出力する端末インタフェース部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と

を備えたことを特徴とする。

【0019】

上記秘匿・完全性保証処理部は、

無線通信制御部から制御信号を入力し、入力した制御信号に基づいて無線通信部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

秘匿処理したデータを端末インタフェース部に出力することを特徴とする。

【0020】

上記無線通信部は、透過データと非透過データとを出力し、

上記無線通信制御部は、非透過データを無線通信部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを無線通信部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする。

【0021】

上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする。

【0022】

上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする。

【0023】

上記秘匿・完全性保証処理部は、
入力したデータを復号化する復号化部を有する秘匿処理部と、
入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部を有する完全性保証処理部と
を備えたことを特徴とする。

【0024】

上記秘匿処理部は、複数の復号化部を有することを特徴とする。

【0025】

上記完全性保証処理部は、複数の完全性確認部を有することを特徴とする。

【0026】

上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する1つのモジュールであり、その1つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行することを特徴とする。

【0027】

この発明に係る無線通信装置は、データを無線通信する無線通信装置において、
データを入出力する端末インタフェース部と、

プロトコルに基づいてデータの処理をする無線通信制御部と、
データを無線通信する無線通信部と、

端末インタフェース部と無線通信制御部と無線通信部との三者間に設けられ、
無線通信制御部との間でデータに対して少なくともデータを暗号化復号化する秘
匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端
末インタフェース部から無線通信部へのデータを暗号化するとともに無線通信部
から端末インタフェース部へのデータを復号する秘匿・完全性保証処理部と
を備えたことを特徴とする。

【0028】

上記秘匿・完全性保証処理部は、
入力したデータに対して秘匿処理を行う秘匿処理部と、
入力したデータに対して完全性保証処理を行う完全性保証処理部と
を個別に備えたことを特徴とする。

【0029】

上記秘匿処理部は、
端末インタフェース部から無線通信部へのデータを暗号化する暗号化部と、
無線通信部から端末インタフェース部へのデータを復号化する復号化部とを個
別に有することを特徴とする。

【0030】

上記完全性保証処理部は、
入力したデータに対して完全性保証処理を行う完全性認証子を付加する完全性
認証子付加部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を
確認する完全性確認部と
を個別に有することを特徴とする。

【0031】

上記通信装置は、携帯型移動電話機であることを特徴とする。

【0032】

【発明の実施の形態】

実施の形態 1.

図 1 は、この実施の形態の移動体通信システムの全体構成図である。

無線端末 (MS) 100 は、この発明の無線通信装置の一例である。無線端末 (MS) 100 は、無線で無線基地局 (BTS) 110 と接続される。無線基地局 (BTS) 110 は、無線制御局 (RNC) 120 と接続される。無線制御局 (RNC) 120 は、他の無線制御局 (RNC) 120 と接続される。また、無線制御局 (RNC) 120 は、コアネットワーク (CN) 130 に接続され、コアネットワーク (CN) 130 を介して他の無線制御局 (RNC) 120 と接続される。

【0033】

図 2 は、図 1 と同じ移動体通信システムの構成図である。特に、無線制御局 (RNC) 120 の内部の構成を示している。

BTS IF 部 121 は、無線基地局 (BTS) 110 を接続する。ハンドオーバー制御部 122 は、無線基地局 (BTS) 110 間を無線端末 (MS) 100 が移動する場合のハンドオーバーを制御する。

【0034】

対 MS 信号制御部 123 は、無線端末 (MS) 100 との間での無線通信制御及びデータの秘匿処理／完全性保証処理を行う。以下に述べる無線端末 (MS) 100 の秘匿処理及び完全性保証処理は、対 MS 信号制御部 123 の秘匿処理及び完全性保証処理に対応して行われるものである。即ち、無線端末 (MS) 100 において暗号化されたデータは、対 MS 信号制御部 123 において復号化される。逆に、対 MS 信号制御部 123 で暗号化されたデータは、無線端末 (MS) 100 において復号化される。また、無線端末 (MS) 100 においてデータの完全性を保証するために付加された認証子は、対 MS 信号制御部 123 において検証される。逆に、対 MS 信号制御部 123 においてデータの完全性を保証するために付加された認証子は、無線端末 (MS) 100 において検証される。この無線端末 (MS) 100 と対 MS 信号制御部 123 におけるデータの秘匿処理及びデータの完全性保証処理は、OSI の 7 つの階層の内の 2 番目のレイヤ、即ち、レイヤ 2 (データリンク層) で行われる。CN IF 部 124 は、コアネット

ワーク (CN) 130とのインタフェースをとる。

【0035】

RNC IF部125は、他の無線制御局 (RNC) 120とのインタフェースをとる。対CN信号制御部126は、コアネットワーク (CN) 130との間での制御を行う。対RNC信号制御部127は、他の無線制御局 (RNC) 120との間で制御を行う。制御部128は、無線制御局 (RNC) 120全体を制御する。スイッチ129は、制御部128の制御に基づいて、無線基地局 (BTS) 110と無線制御局 (RNC) 120とコアネットワーク (CN) 130との間で制御信号並びにパケットデータをスイッチングする。即ち、スイッチ129は、パケットデータだけでなく、音声等を含む全てのデータをスイッチするとともに、制御信号もスイッチする。

【0036】

図3は、無線端末 (MS) 100の構成図である。

無線端末 (MS) 100は、端末IF部10と無線通信制御部20と無線通信部30と秘匿・完全性保証処理部40を有している。端末IF部10は、カメラ1とビデオ2とB/T (Blue Tooth) 3とLCD4とKEY5とLED6とUSIM (Universal Subscriber Identity Module) 7とRECEIVER8とMIC9とHSJ (Head Set Jack) 0とを接続している。これらのカメラ1からHSJ0は、ユーザ (人間) もしくは接続の対象となる機器とのインターフェースのための処理を行い、ユーザ (人間) もしくは接続の対象となる機器が認識できる情報を入力又は出力するものである。

【0037】

端末IF部10は、内部に各モジュールIF部11とデータフォーマット変換部12と端末IF制御部13と音声符号化/復号化部14を有している。各モジュールIF部11は、カメラ1からHSJ0との各インタフェースをとる。データフォーマット変換部12は、カメラ1からHSJ0で取り扱う各データフォーマットと無線端末 (MS) 100内部で取り扱う各データフォーマットとの間での変換を行う。端末IF制御部13は、端末IF部10の動作を制御する。音声

符号化／復号化部 14 は、MIC 9 から入力された音声電気信号を音声符号化する。また、音声符号化／復号化部 14 は、音声符号化された信号を復号して RECEIVER 8 に対して音声電気信号を出力する。

【0038】

無線通信制御部 20 は、無線端末 (MS) 100 の全体制御を行う。無線通信制御部 20 には、CPU、ROM、RAM、ファームウェア等からなるハードウェア回路、或いは、ソフトウェアモジュールが備えられている。無線通信制御部 20 は、端末 IF 部 10 と無線通信部 30 との間でデータを処理するものであり、規格或いはプロトコルにより定められた規則に基づいてデータの変換処理を行う。特に、レイヤ 2 以上の処理を行う。例えば、データの packets 化やデータの連結等を行う。無線通信制御部 20 は、レイヤ 2 以上のデータを取り扱うため、データの種別を判断することができる。そして、データの種別に応じて、そのデータが秘匿処理されるべきデータであるか、又は、完全性保証処理されるべきデータであるかを判断することができる。レイヤ 1 のデータでは、データの種別を判断できないため、そのデータが秘匿処理されるべきデータであるか、又は、完全性保証処理されるべきデータであるかを判断することができない。

【0039】

無線通信部 30 は、通信路符号化部 310 とベースバンド変復調部 320 と無線部 330 とアンテナ 34 を備えている。通信路符号化部 310 は、各通信路用の符号化部と復号化部を有している。符号化部として、誤り検出符号化部 311 と誤り訂正符号化部 312 と物理フォーマット変換部 313 を有している。また、復号化部として物理フォーマット変換部 314、誤り訂正復号化部 315、誤り検出部 316 を有している。ベースバンド変復調部 320 は、帯域の変調及び復調を行う。ベースバンド変復調部 320 は、ベースバンド変調部 321 とベースバンド復調部 322 を有している。無線部 330 は、ベースバンド帯域の信号を伝送帯域に変換もしくは伝送帯域の信号をベースバンド帯域に変換する。無線部 330 は、アップコンバータ 331 とダウンコンバータ 332 を有している。

【0040】

秘匿・完全性保証処理部 40 は、無線通信制御部 20 に接続されている。秘匿

・完全性保証処理部 40 は、無線通信制御部 20 からデータを受け取り、秘匿処理を行う。また、データの完全性保証処理を行う。秘匿・完全性保証処理部 40 は、無線通信制御部 20 から秘匿及び完全性保証処理のための制御信号 91 を入力する。また、秘匿・完全性保証処理部 40 は、無線通信制御部 20 からレイヤ 2 以上の任意の階層における秘匿処理の対象となるデータ及び／又は完全性保証処理の対象となるデータ 92 を入力する。秘匿・完全性保証処理部 40 は、入力した制御信号 91 に基づいてデータ 92 に対して秘匿処理及び／又は完全性保証処理を行い、無線通信制御部 20 に出力する。制御信号 91 の中には、鍵や初期値や秘匿処理と完全性保証処理との選択等のパラメータが含まれている。

【0041】

図 4 は、秘匿・完全性保証処理部 40 の構成図である。

秘匿・完全性保証処理部 40 は、IF 部 410 と 1 つのモジュール 411 を有している。モジュール 411 は、秘匿処理と完全性保証処理を 1 つの同一の回路又は 1 つの同一のアルゴリズムで行うものである。秘匿処理を行うか、完全性保証処理を行うかは、制御信号 91 により決定される。ここで、秘匿処理とは、データを暗号化、或いは、復号化することをいう。また、完全性保証処理とは、データの改竄の有無を検証するために、データに対して認証子を付加する処理、或いは、認証子を再生して比較することによりデータの改竄の有無を判定する処理のことをいう。秘匿処理と完全性保証処理は、同一の回路又は同一のアルゴリズム、或いは、類似の回路又は類似のアルゴリズムを用いて行うことができるため、図 4 に示すように、秘匿処理と完全性保証処理を 1 つのモジュール 411 で行うことが可能である。図 4 に示す場合は、ハードウェアリソース及びソフトウェアリソースの削減が可能である。以下、モジュールとは、ハードウェアのみで実現されるもの、ソフトウェアのみで実現されるもの、ハードウェアとソフトウェアとの組み合わせで実現されるもののいずれかをいうものとする。

【0042】

図 5 は、秘匿・完全性保証処理部 40 の他の例を示す図である。

図 5 において特徴となる点は、秘匿処理部 420 と完全性保証処理部 430 を個別に設けた点である。秘匿処理部 420 の内部には、暗号化／復号化部 421

が設けられている。完全性保証処理部 430 の内部には、完全性認証子付加／完全性確認部 431 が設けられている。暗号化／復号化部 421 は、暗号化と復号化を 1 つの同一モジュールを用いて行う場合を示している。完全性認証子付加／完全性確認部 431 は、完全性認証子の付加と完全性の確認を 1 つの同一のモジュールで行う場合を示している。図 5 に示す場合は、暗号化と復号化が同じ関数であった場合及び完全性認証子付加と完全確認が同じ関数であった場合に、取り得る構成である。図 5 に示す場合は、図 6 に示す場合に比べ、ハードウェアリソース及びソフトウェアリソースの削減が可能である。

【0043】

図 6 は、秘匿・完全性保証処理部 40 の他の構成を示す図である。

図 6 の特徴は、秘匿処理部 420 において、暗号化部 422 と復号化部 423 を個別に設けた点である。また、完全性保証処理部 430 において、完全性認証子付加部 432 と完全性確認部 433 を個別に設けた点である。図 6 に示す場合は、暗号化と復号化が同じ又は違う関数であった場合及び完全性認証子付加と完全性確認が同じ又は違う関数であった場合を取る構成である。図 6 の場合は、暗号化、復号化、完全性認証子付加、完全性確認を個別に実行でき、送受信されるデータが同時並列に秘匿処理、或いは、完全性保証処理されるので、処理の高速化が可能である。

【0044】

図 7 は、秘匿処理部 420 において、複数の暗号化部 422 と複数の復号化部 423 を設けた場合を示している。また、完全性保証処理部 430 において、複数の完全性認証子付加部 432 と複数の完全性確認部 433 を設けた場合を示している。無線端末 (MS) 100 が動作している場合に、複数のチャネルが同時に処理されなければならない場合がある。例えば、音声とファクシミリデータの 2 種類のデータが同時に伝送されるような場合には、少なくとも 2 チャネルのデータが同時に処理される必要がある。このような場合には、音声データを暗号化部 1 で暗号化し、ファクシミリデータを暗号化部 2 で暗号化することができる。また、復号する場合にも、同時に複数チャネルのデータを復号化することができる。暗号化部 422 と復号化部 423 と完全性認証子付加部 432 と完全性確認

部 4 3 3 の数 (図 7 では、 n 個) は、全て同一である必要はなく、無線端末 (MS) 1 0 0 において同時に処理すべきチャネルの数に応じて各部分の数を決定すればよい。或いは、各チャネルに対応するのではなく、ある 1 つのチャネルに大量データの高速処理を行う必要が生じた場合に、その 1 つのチャネルに割り当てられた大量データを 2 つの暗号化部により処理するようにしても構わない。即ち、~~暗号化部 4 2 2 と復号化部 4 2 3 と完全性認証子付加部 4 3 2 と完全性確認部 4 3 3 の各部の数は、同時に処理すべきチャネルの数及び／又はデータ量により決定すればよい。~~

【0 0 4 5】

図 8 は、秘匿処理部 4 2 0 に複数の暗号化／復号化部 4 2 1 を設けた場合を示している。また、完全性保証処理部 4 3 0 に複数の完全性認証子付加／完全性確認部 4 3 1 を設けた場合を示している。

図 8 は、図 5 に示す暗号化／復号化部 4 2 1 と完全性認証子付加／完全性確認部 4 3 1 を複数にしたものである。図 8 に示す場合は、暗号化と復号化が同じ関数であった場合に、複数のチャネルに対応して複数の暗号化／復号化部 4 2 1 を設けた場合を示している。同様に、完全性認証子付加と完全性確認が同じ関数であった場合に、複数のチャネルに対応して完全性認証子付加／完全性確認部 4 3 1 を複数設けた場合を示している。図 8 の場合は、図 7 の場合に比べて、ハードウェアリソース及びソフトウェアリソースの削減を行うことが可能である。

図 4 から図 8 においては、秘匿・完全性保証処理部 4 0 が秘匿処理部 4 2 0 と完全性保証処理部 4 3 0 とを両方備えている場合を示したが、秘匿・完全性保証処理部 4 0 が秘匿処理部 4 2 0 又は完全性保証処理部 4 3 0 のいずれか片方だけ備えている場合でもよい。秘匿・完全性保証処理部 4 0 が秘匿処理部 4 2 0 又は完全性保証処理部 4 3 0 の一方だけ備えている場合は、他方の処理は、無線通信制御部 2 0 が行えばよい。

【0 0 4 6】

実施の形態 2.

図 9 は、無線端末 (MS) 1 0 0 の他の例を示す構成図である。

図 9 が図 3 と異なる点は、端末 IF 部 1 0 と秘匿・完全性保証処理部 4 0 との

間でデータの入出力が行われる点である。また、無線通信部 3 0 と秘匿・完全性保証処理部 4 0 との間でデータの入出力が行われる点である。図 9 において、非透過データ 9 7 は、パケットデータ等の非透過データである。また、透過データ 9 5, 9 6 は、音声データや非制限デジタルデータ等の透過データである。透過データとは、あるレイヤ、或いは、あるレイヤのサブレイヤにおいて、入力から出力まで、そのデータが一切変更されないデータをいう。一方、非透過データとは、あるレイヤ、或いは、あるレイヤのサブレイヤにおいて、入力から出力まで、そのデータのフォーマット変換処理等の何等かのデータ処理が必要なデータをいう。例えば、レイヤ 2 の R L C (R a d i o L i n k C o n t r o l) サブレイヤにおいて、S D U (S e r v i c e D a t a U n i t) と P D U (P r o t o c o l D a t a U n i t) とが異なる場合は、そのデータは非透過データであり、レイヤ 2 の M A C (M e d i a A c c e s s C o n t r o l) サブレイヤにおいて、S D U と P D U が同一の場合、そのデータは透過データである。図 9 に示す場合は、無線通信部 3 0 との間で入出力されるレイヤ 1 のデータに対して何等処理を行うことなく、端末 I F 部 1 0 に引き渡すことができるデータ、例えば、音声データを、透過データとしている。一方、無線通信部 3 0 から出力されるレイヤ 1 のデータに対して何等かの処理を行わなければならないデータ、例えば、パケットデータを、非透過データとしている。図 9 に示す秘匿・完全性保証処理部 4 0 は、無線通信制御部 2 0 との間で非透過データに対して秘匿処理と完全性保証処理を選択的に行うとともに、端末 I F 部 1 0 と無線通信部 3 0 との間で入出力される透過データに対して、例えば、秘匿処理を必ず行うものである。秘匿・完全性保証処理部 4 0 は、透過データに対しては完全性保証処理を行わない。もし、透過データのなかに秘匿処理を行いたくないものがある場合には、無線通信制御部 2 0 は、その秘匿処理を行いたくない透過データを秘匿・完全性保証処理部 4 0 に入力させず無線通信制御部 2 0 に入力させればよい。或いは、その秘匿処理を行いたくない透過データを秘匿・完全性保証処理部 4 0 に入力させるが、無線通信制御部 2 0 からの制御信号を用いてその透過データに秘匿処理を行わせないようにしてもよい。

【 0 0 4 7 】

図10は、秘匿・完全性保証処理部40の構成図である。

図10において、図5と異なる点は、新たに秘匿処理部460が設けられた点である。秘匿処理部460には、暗号化部462と復号化部463が設けられている。暗号化部462は、端末IF部10からの透過データ95を入力し、入力したデータを暗号化し、制御信号96として無線通信部30へ出力する。一方、~~復号化部463は、無線通信部30から透過データ96を入力し、復号化し、透過データ95として端末IF部10へ出力する。~~秘匿処理部460のこれらの処理は、IF部410からの制御信号99に基づいて行われる。制御信号99は、制御信号91から生成された制御信号である。従って、秘匿処理部460は、無線通信制御部20からの制御信号に基づいて秘匿処理を行うことになる。図10において、データ92は、バスを介したパラレルインタフェースを用いて入出力される。一方、透過データ95と96は、シリアルインタフェースを介して秘匿処理部460に対して入出力される。このように、図10は、秘匿・完全性保証処理部40がパラレルインタフェースとシリアルインタフェースの2系統の入出力インタフェースを備えている場合を示している。

【0048】

図11は、図7に示した秘匿・完全性保証処理部40の構成に秘匿処理部460を付加した場合を示している。図11に示すような秘匿処理部460の構成は、図12に示すように、暗号化部又は復号化部がキーストリームを発生させ、シリアルデータと排他的論理和をとる場合に有効な構成である。

図11は、透過データ95、96がシリアルインタフェースを介して秘匿処理部460に入出力される場合であって、かつ、そのシリアルインタフェースを介して入出力されるシリアルデータに、複数チャネルのデータが多重化されている場合を示している。例えば、チャネル1のデータの次にチャネル2のデータがシリアルデータとして入力された場合、チャネル1に対応する暗号化部1からキーストリームを発生させデータ多重部481に出力し、チャネル2に対応する暗号化部2からキーストリームを発生させデータ多重部481に出力し、データ多重部481において、これらのキーストリームを入力されるデータ95のデータ系列と同じフォーマットに多重する。この多重したキーストリームと入力されるデ

ータ 95 のデータ系列との排他的論理和を排他的論理和回路 483 により演算する。秘匿処理部 460 のこれらの動作は制御信号 99 に基づいて、即ち、無線通信制御部 20 から送られてきた制御信号 91 に基づいて行われる。図 11 の構成によれば、シリアルデータの遅延が排他的論理和回路 483 の演算のみで済み、高速な処理を行うことが可能である。

【0049】

図 13 は、図 10 の秘匿処理部 420 と秘匿処理部 460 とをあわせて 1 つの秘匿処理部 470 とした場合を示している。

秘匿処理部 470 は、パラレルインタフェースから入出力されるデータ 92 とシリアルインタフェースから入出力されるデータ 95、96 の両方を処理する。470 は、秘匿処理部 420 と秘匿処理部 460 を 1 つにまとめたものであるため、ハードウェアリソースの削減が可能である。秘匿処理部 470 における透過データと非透過データの処理動作のスイッチングは、制御信号 99、即ち、無線通信制御部 20 から出力された制御信号 91 に基づいて行われる。

【0050】

前述した秘匿・完全性保証処理部 40 は、ハードウェアで構成することができる。例えば、FPGA やカスタム LSI で実現することができる。また、秘匿・完全性保証処理部 40 は、ソフトウェアプログラムで実現することもできる。秘匿・完全性保証処理部 40 がソフトウェアプログラムで実現される場合、ソフトウェアプログラムは無線通信制御部 20 にある CPU により実行されることになる。

また、秘匿・完全性保証処理部 40 は、ハードウェアとソフトウェアの組み合わせにより実現することができる。例えば、DSP (Digital Signal Processor) とその DSP により実行されるマイクロプログラムやファームウェアプログラムにより実現することができる。

【0051】

また、前述した例においては、無線通信制御部 20 と秘匿・完全性保証処理部 40 がバスを介したパラレルインタフェースでつながれている場合を示したが、シリアルインタフェースを用いても構わない。また、端末 IF 部 10 と秘匿・完

全性保証処理部 4 0 及び無線通信部 3 0 と秘匿・完全性保証処理部 4 0 がシリアルインタフェースで接続される場合を示したが、より高速な処理を行うためには、シリアルインタフェースではなく、パラレルインタフェースを用いても構わない。

【0052】

また、図 9、図 1 0 においては、秘匿処理部 4 6 0 を秘匿・完全性保証処理部 4 0 の内部に設ける場合を示したが、秘匿処理部 4 6 0 を秘匿・完全性保証処理部 4 0 から外部に独立させて、秘匿処理部 4 6 0 を端末 I F 部 1 0 と無線通信部 3 0 との間に設けてもよい。

【0053】

【発明の効果】

以上のように、前述した実施の形態によれば、レイヤ 1（物理層）において秘匿処理を行わないように、レイヤ 2 以上の階層において秘匿処理及び完全性保証処理を行うようにしたので、データの種別に応じて秘匿処理の可否及び完全性保証処理の可否を決定することができる。

例えば、透過データに対しては秘匿処理のみを行い、非透過データに対して秘匿処理と完全性保証処理の両方を行うことが可能になる。或いは、非透過データであっても秘匿処理と完全性保証処理とをそれぞれ行ったり、行わなかったり選択することが可能になる。

【0054】

また、上記実施の形態によれば、秘匿・完全性保証処理部の内部にチャンネルの数やデータ量に応じて複数の秘匿処理部と複数の完全性保証処理部を設けているので、同時並列処理による高速データ処理が可能となる。

【図面の簡単な説明】

【図 1】 移動体通信システムの構成図。

【図 2】 無線制御局（RNC）1 2 0 の構成図。

【図 3】 実施の形態 1 の無線端末（MS）1 0 0 の構成図。

【図 4】 実施の形態 1 の秘匿・完全性保証処理部 4 0 の構成図。

【図 5】 実施の形態 1 の秘匿・完全性保証処理部 4 0 の構成図。

【図6】 実施の形態1の秘匿・完全性保証処理部40の構成図。

【図7】 実施の形態1の秘匿・完全性保証処理部40の構成図。

【図8】 実施の形態1の秘匿・完全性保証処理部40の構成図。

【図9】 実施の形態2の無線端末(MS)100の構成図。

【図10】 実施の形態2の秘匿・完全性保証処理部40の構成図。

~~【図11】 実施の形態2の秘匿・完全性保証処理部40の構成図。~~

【図12】 暗号化方式及び復号化方式の一例を示す図。

【図13】 実施の形態2の秘匿・完全性保証処理部40の構成図。

【図14】 従来の携帯電話機500を示す図。

【符号の説明】

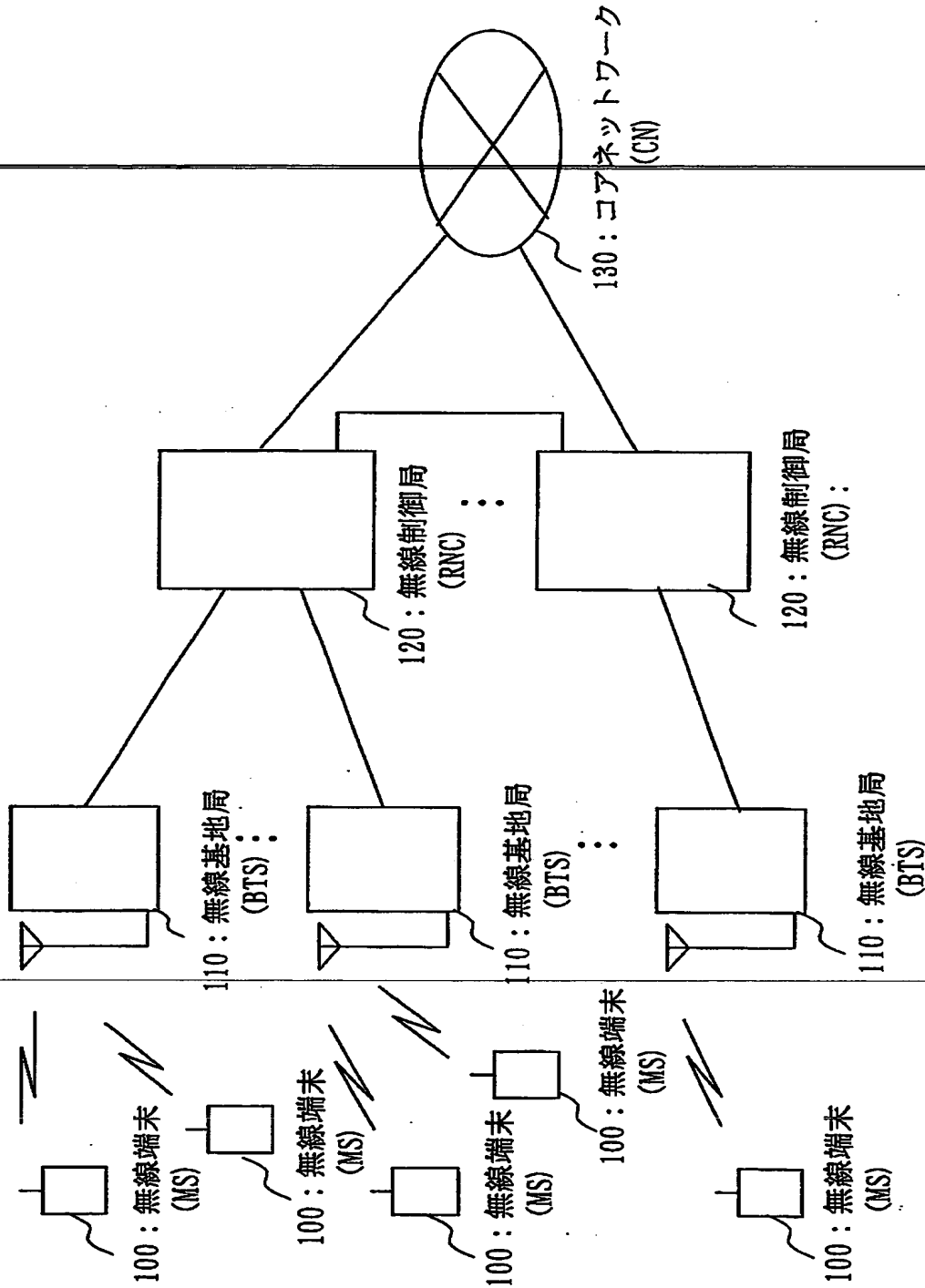
0 HSJ、1 カメラ、2 ビデオ、3 B/T、4 LCD、5 KEY、6 LED、7 USIM、8 RECEIVER、9 MIC、10 端末IF部、11 各モジュールIF部、12 データフォーマット変換部、13 端末IF制御部、14 音声符号化／復号化部、20 無線通信制御部、30 無線通信部、34 アンテナ、40 秘匿・完全性保証処理部、91, 99 制御信号、92～97 データ、100 無線端末(MS: モバイルステーション)、110 無線基地局(BTS: ベーストランシーバステーション)、120 無線制御局(RNC: リモートネットワークコントローラ)、121 BTS IF部、122 ハンドオーバー制御部、123 対MS信号制御部、124 CN IF部、125 RNC IF部、126 対CN信号制御部、127 対RNC信号制御部、128 制御部、129 スイッチ、130 コアネットワーク(CN)、310 通信路符号化部、311 誤り検出符号化部、312 誤り訂正符号化部、313 物理フォーマット変換部、314 物理フォーマット変換部、315 誤り訂正復号化部、316 誤り検出部、320 ベースバンド変復調部、321 ベースバンド変調部、322 ベースバンド復調部、330 無線部、331 アップコンバータ、332 ダウンコンバータ、410 IF部、411 モジュール、420 秘匿処理部、421 暗号化／復号化部、422 暗号化部、423 復号化部、430 完全性保証処理部、431 完全性認証子付加／完全性確認部、432 完全性認証子付加部、433

完全性確認部、4 6 0 秘匿処理部、4 6 2 暗号化部、4 6 3 復号化部、4
7 0 秘匿処理部、4 7 2 暗号化部、4 7 3 復号化部、4 8 1, 4 8 2 デ
ータ多重部、4 8 3, 4 8 4 排他的論理和回路、5 0 0 携帯電話機、5 1 0
端末 I F 部、5 2 0 無線通信制御部、5 3 0 無線通信部、5 4 0 秘匿処
理部、5 4 1 アンテナ。

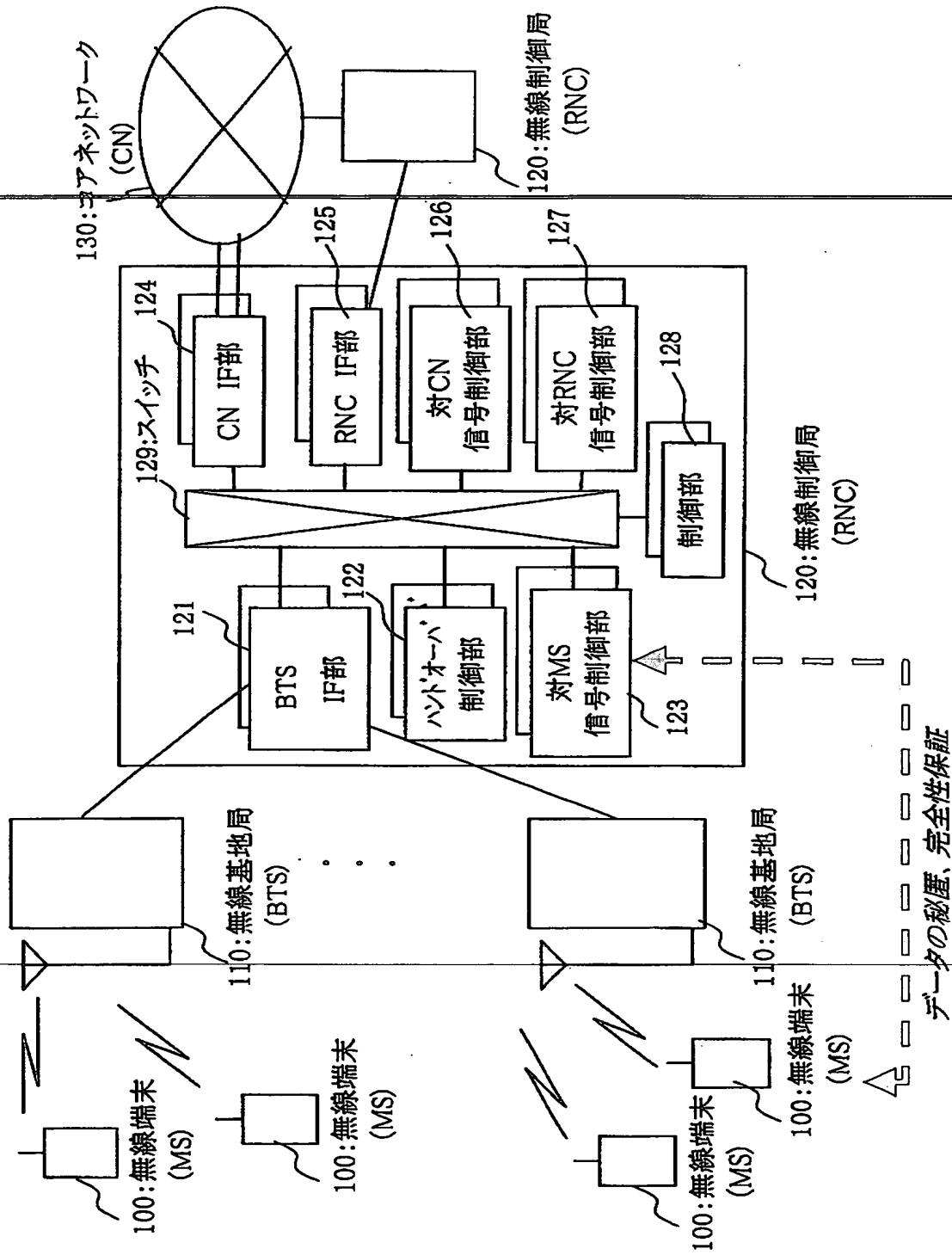
【書類名】

図面

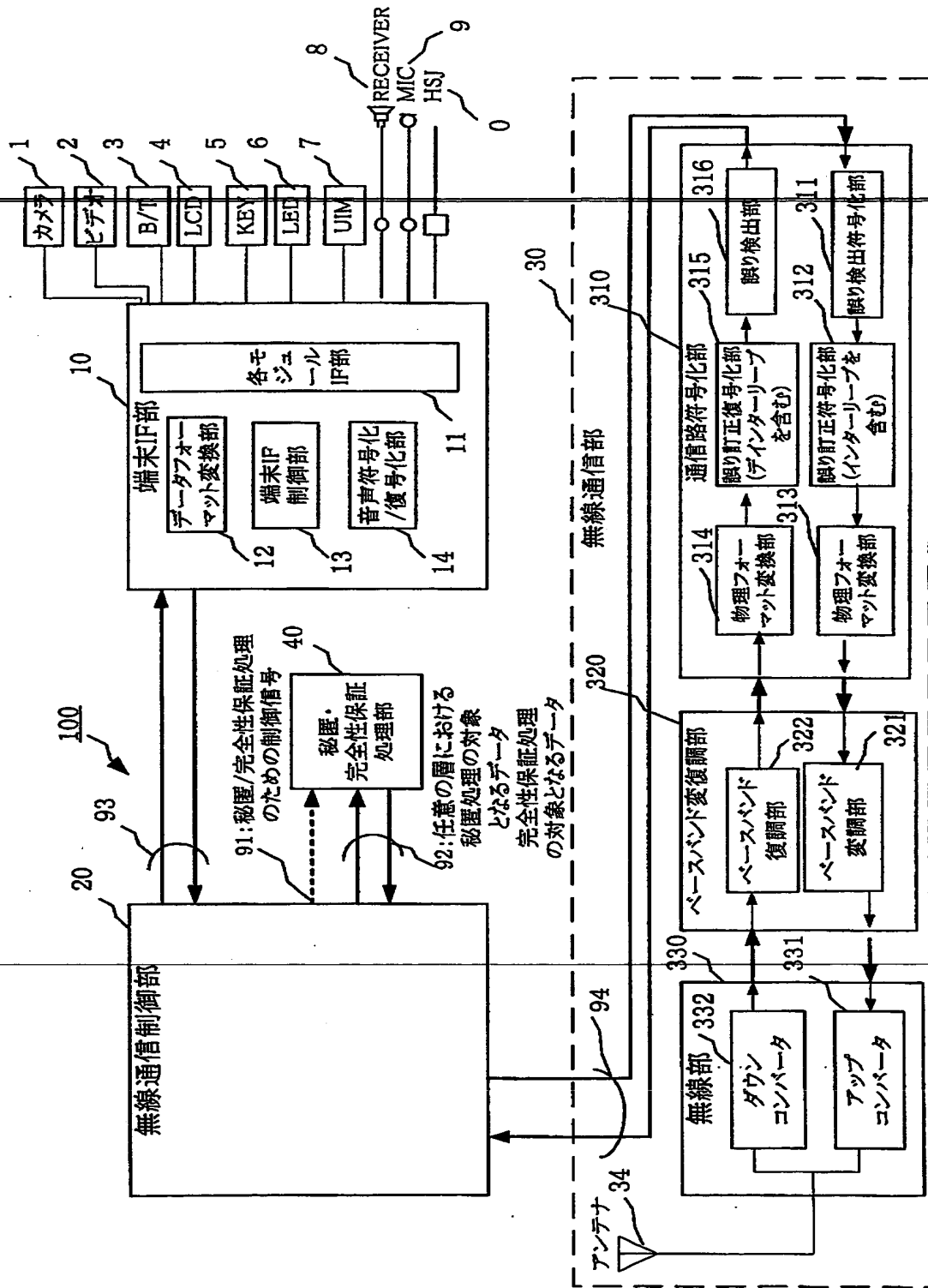
【図 1】



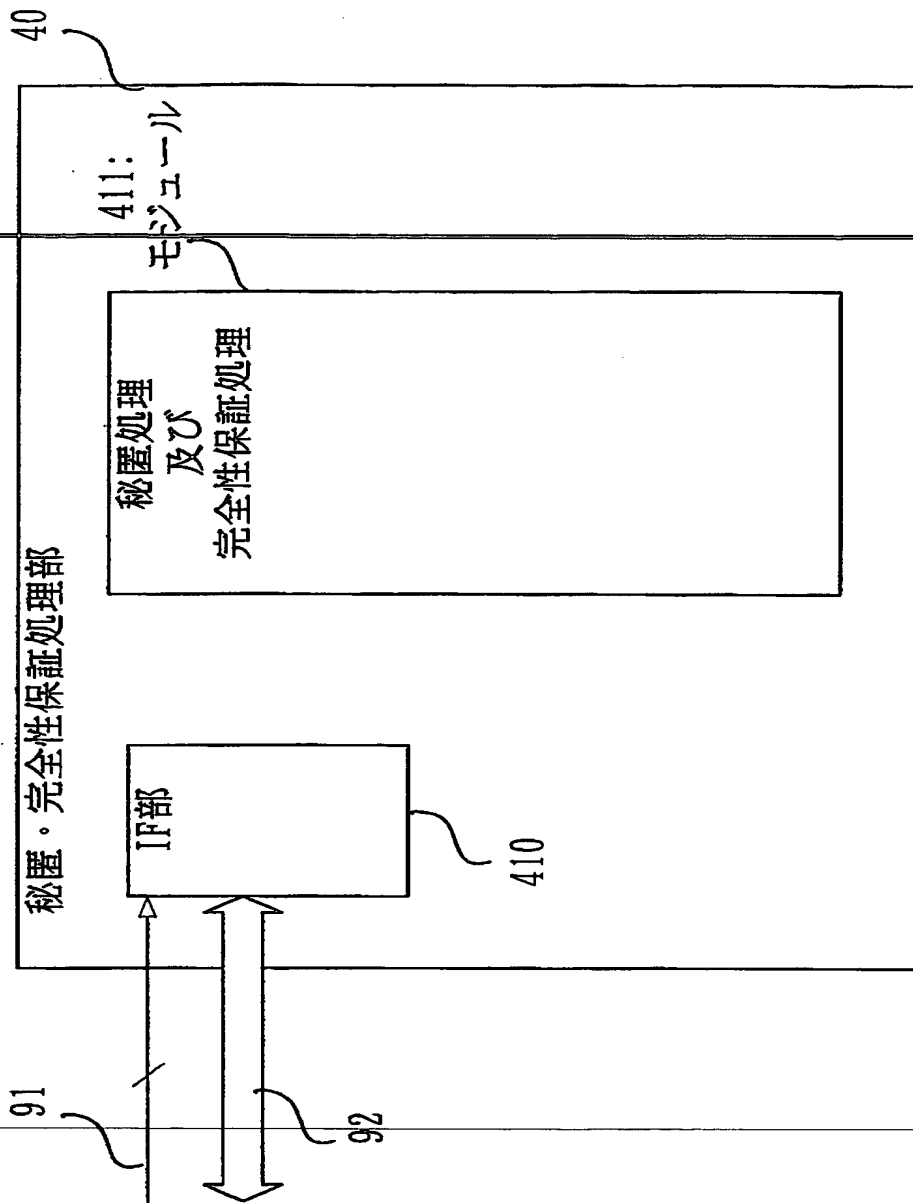
【図2】



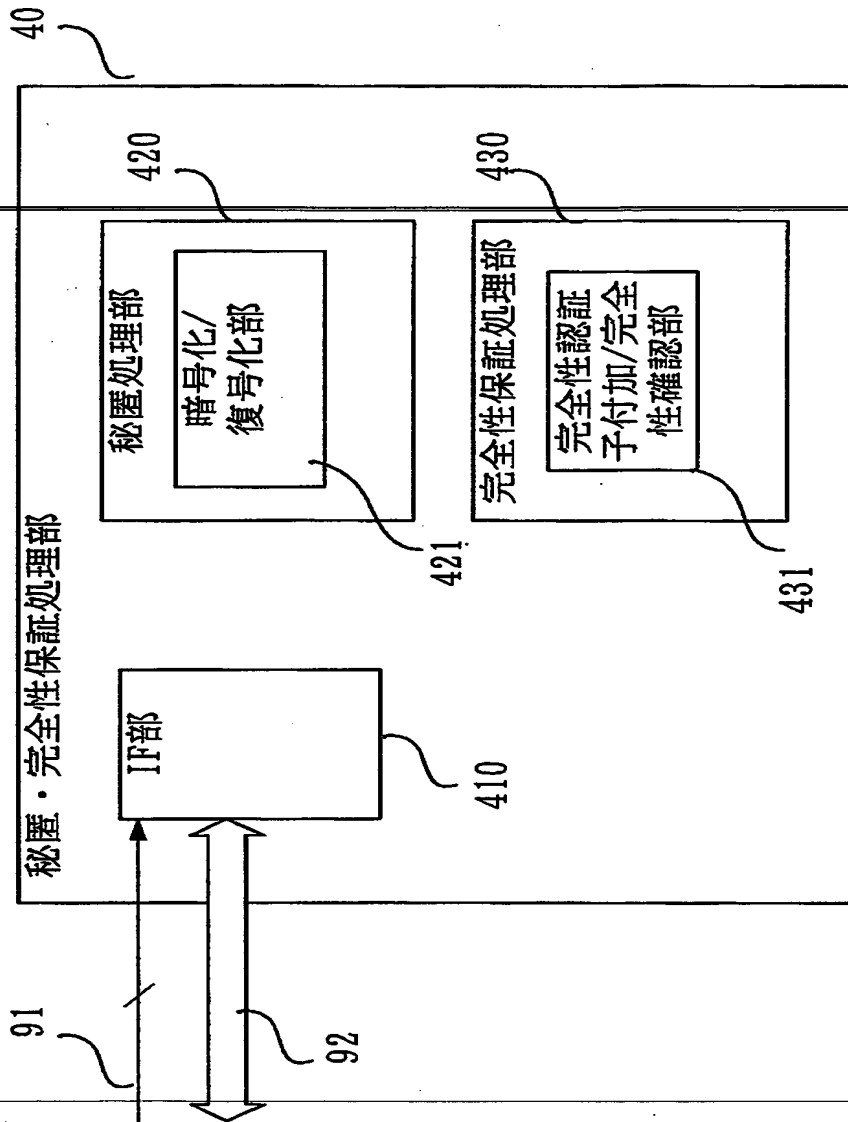
【図 3】



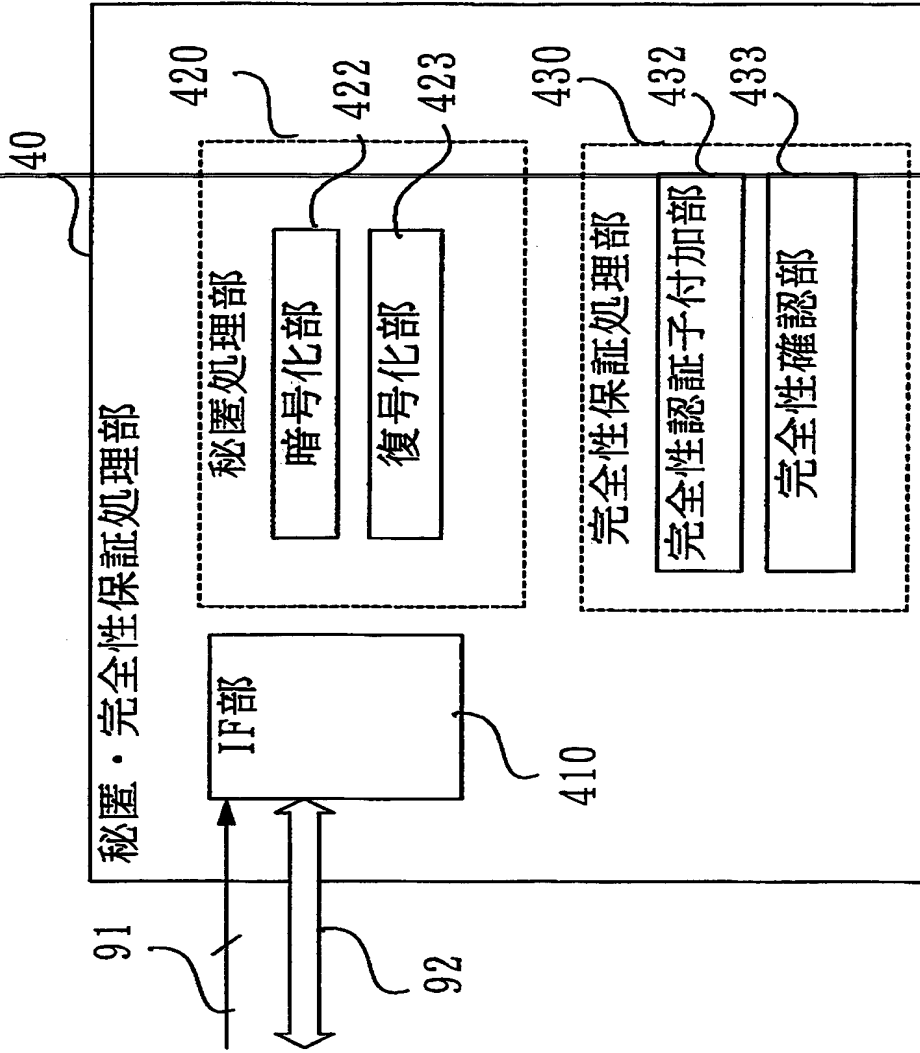
【図 4】



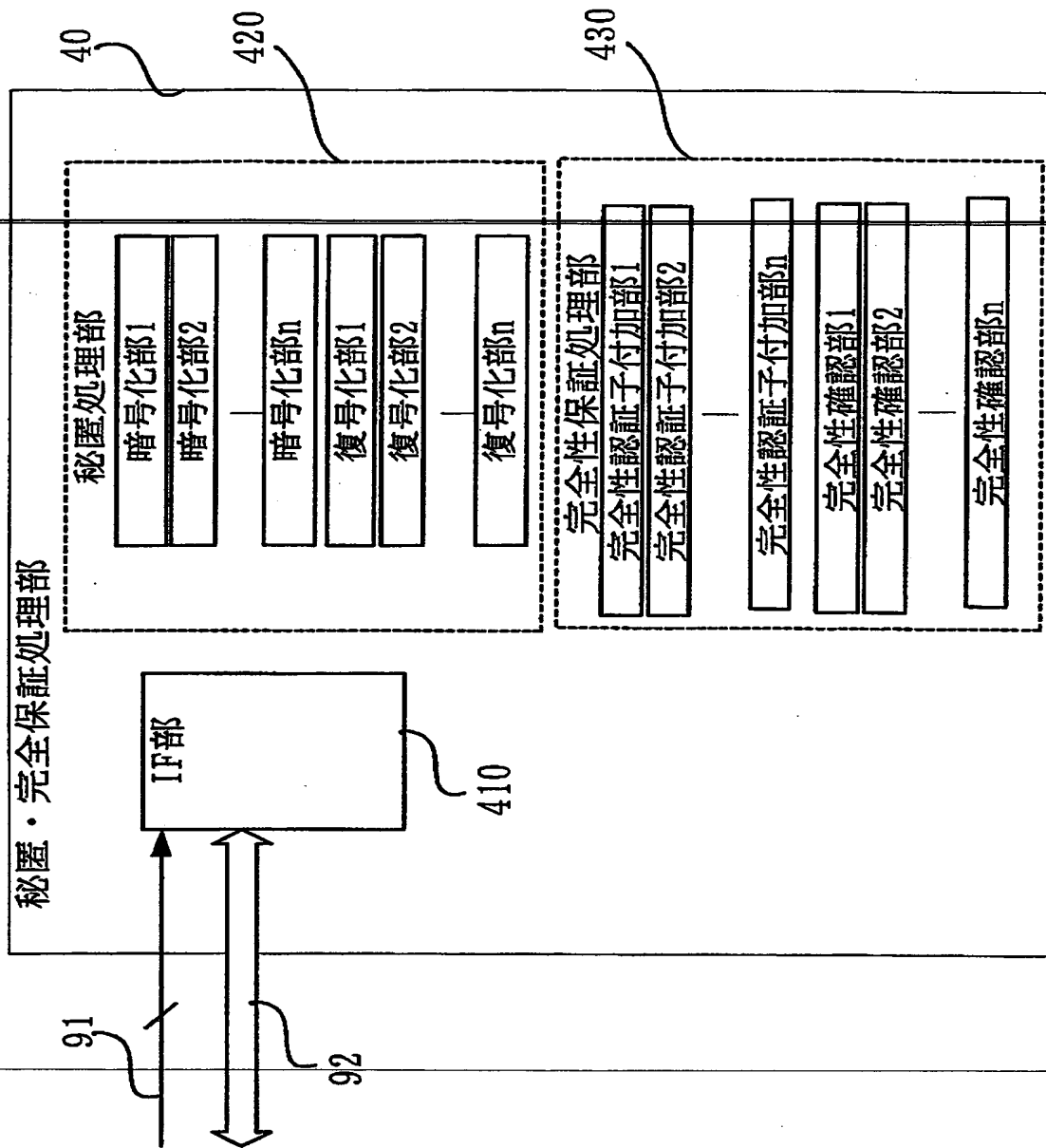
【図 5】



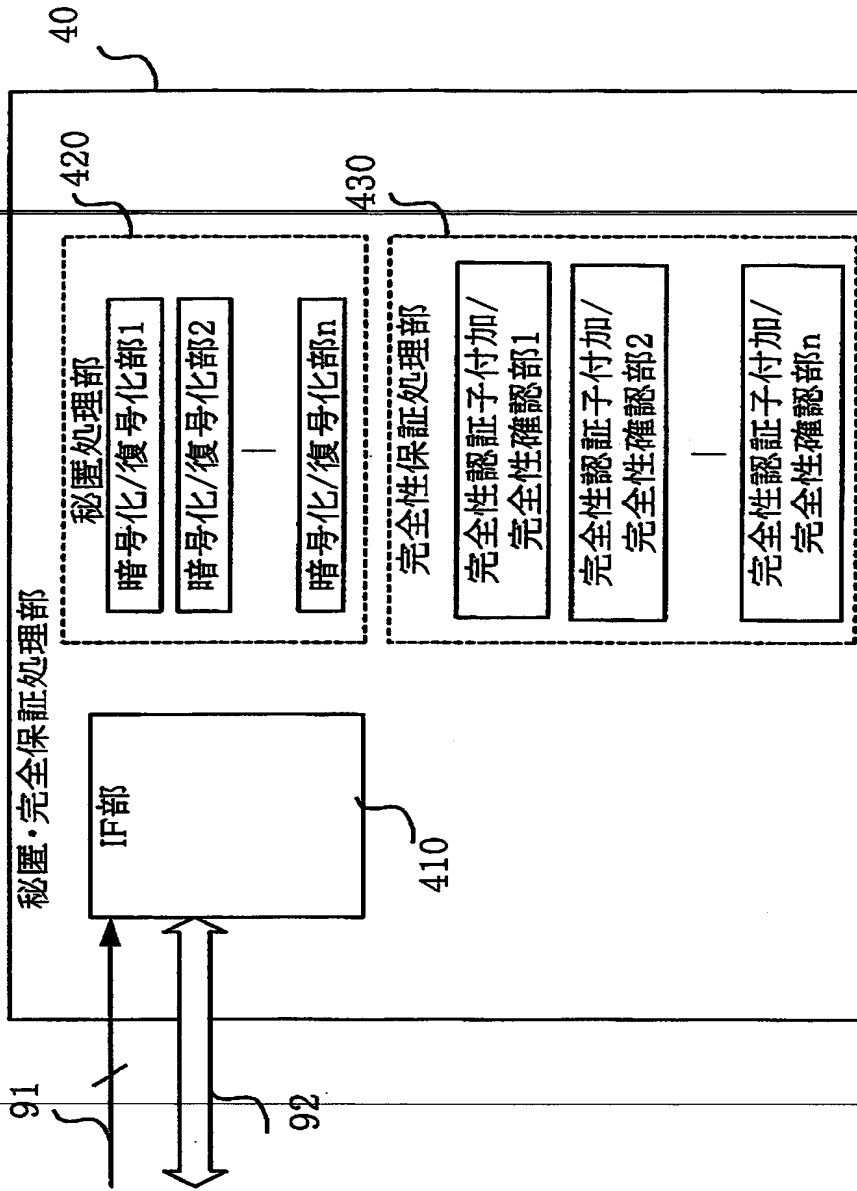
【図 6】



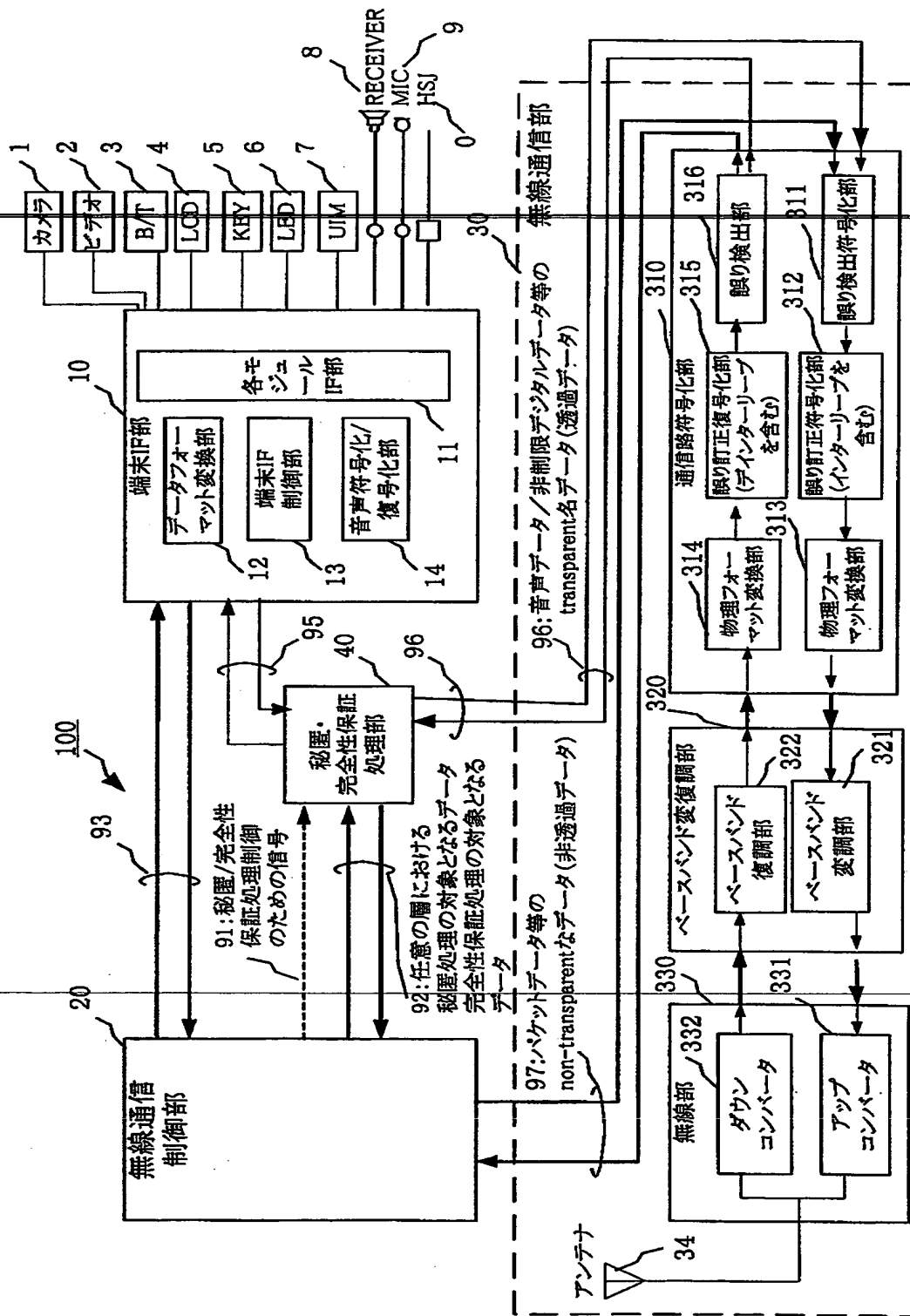
【図 7】



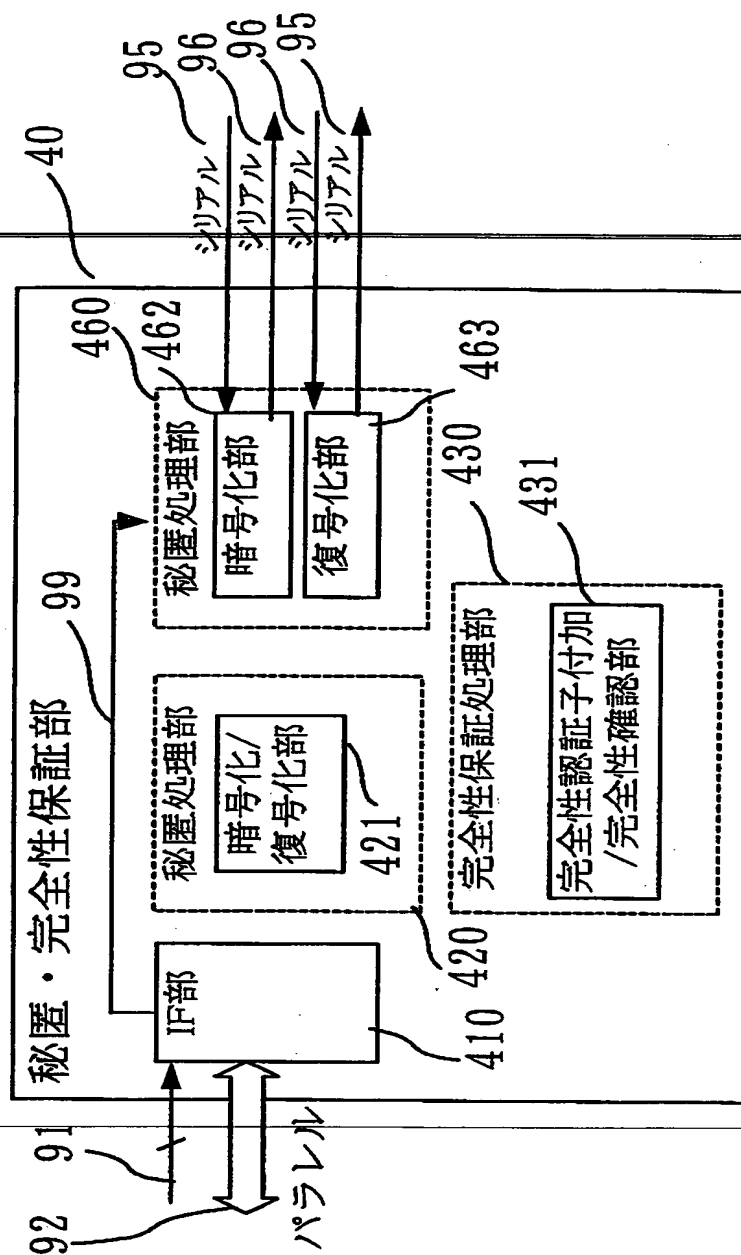
【図 8】



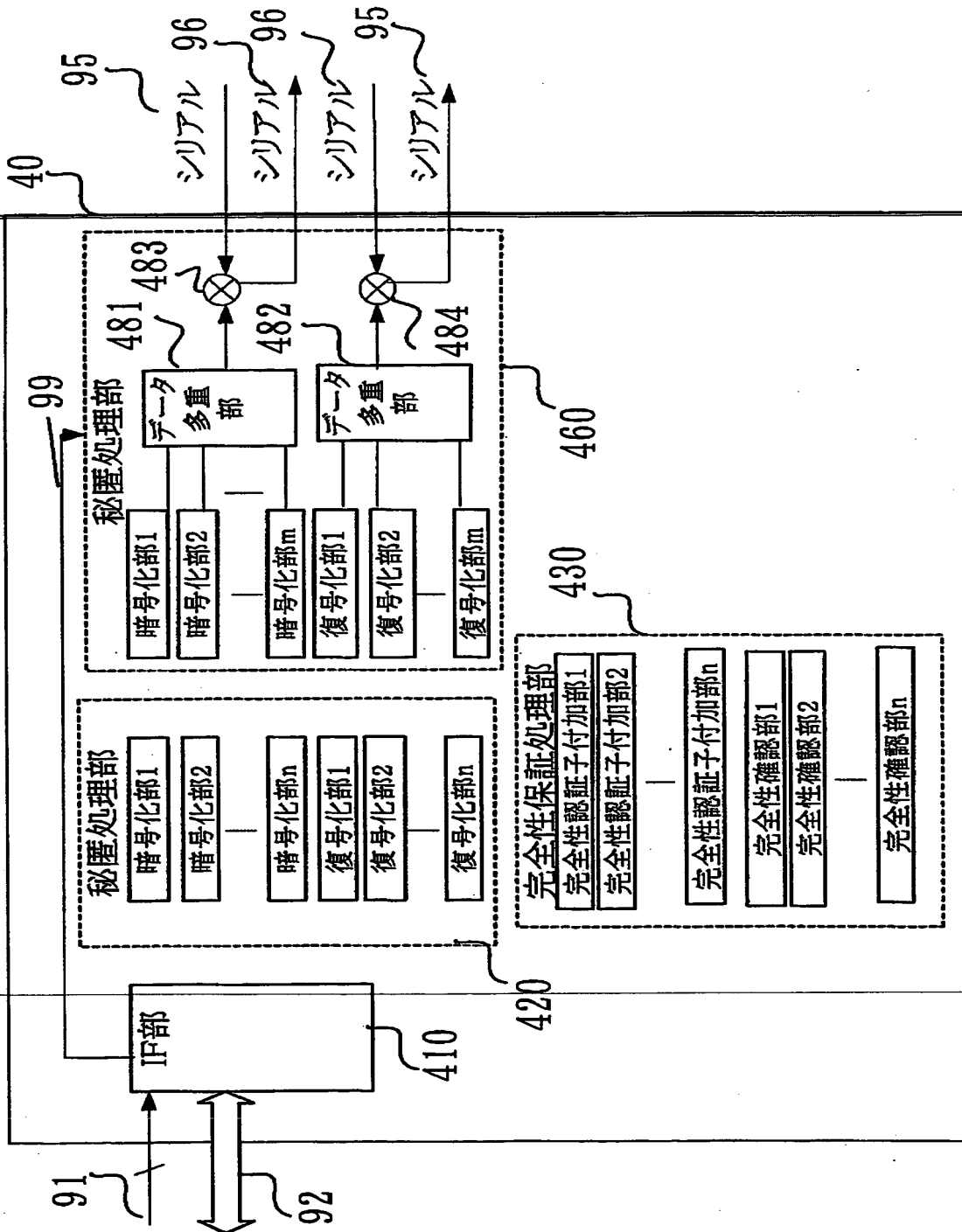
【図 9】



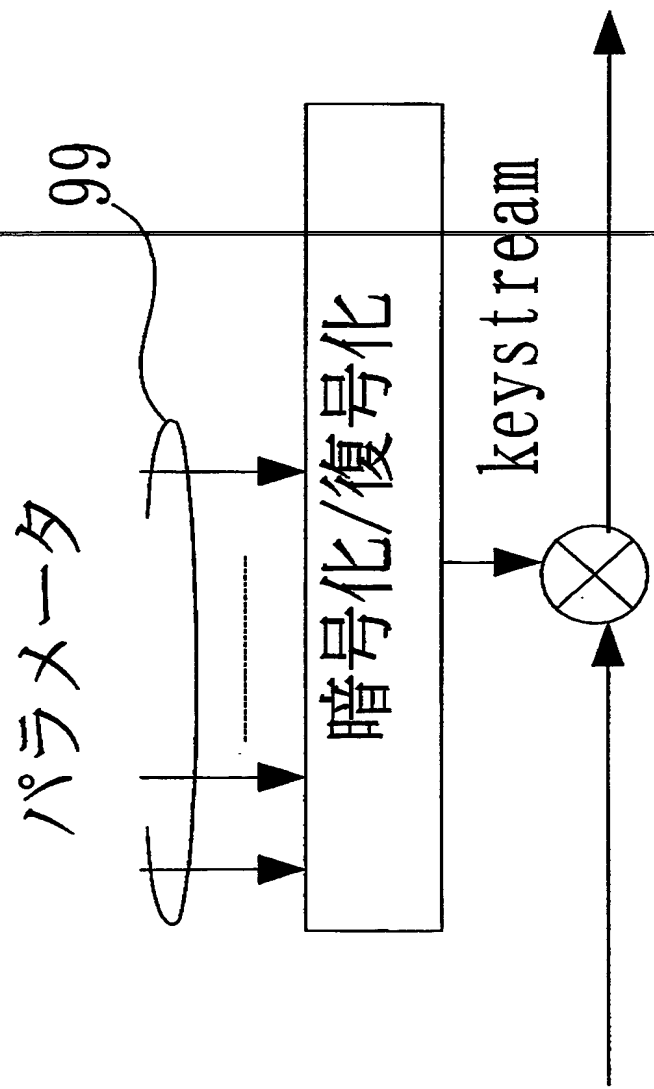
【図 10】



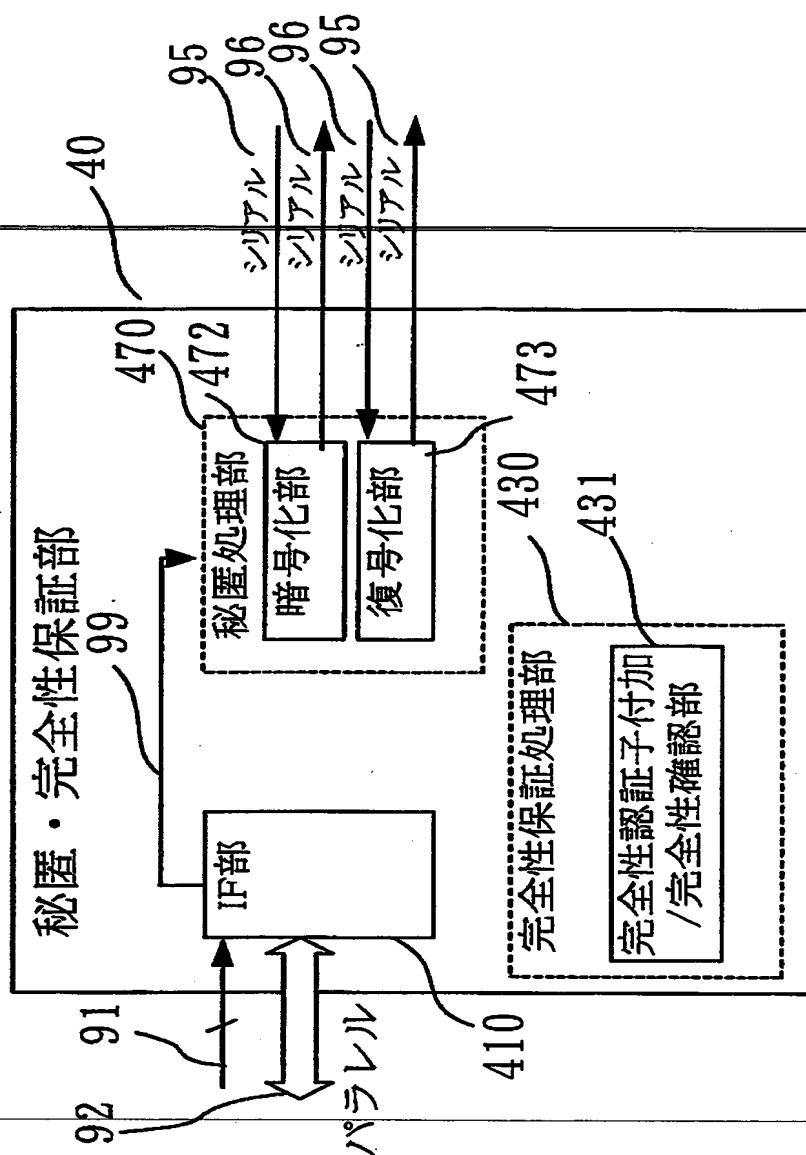
【図 1 1】



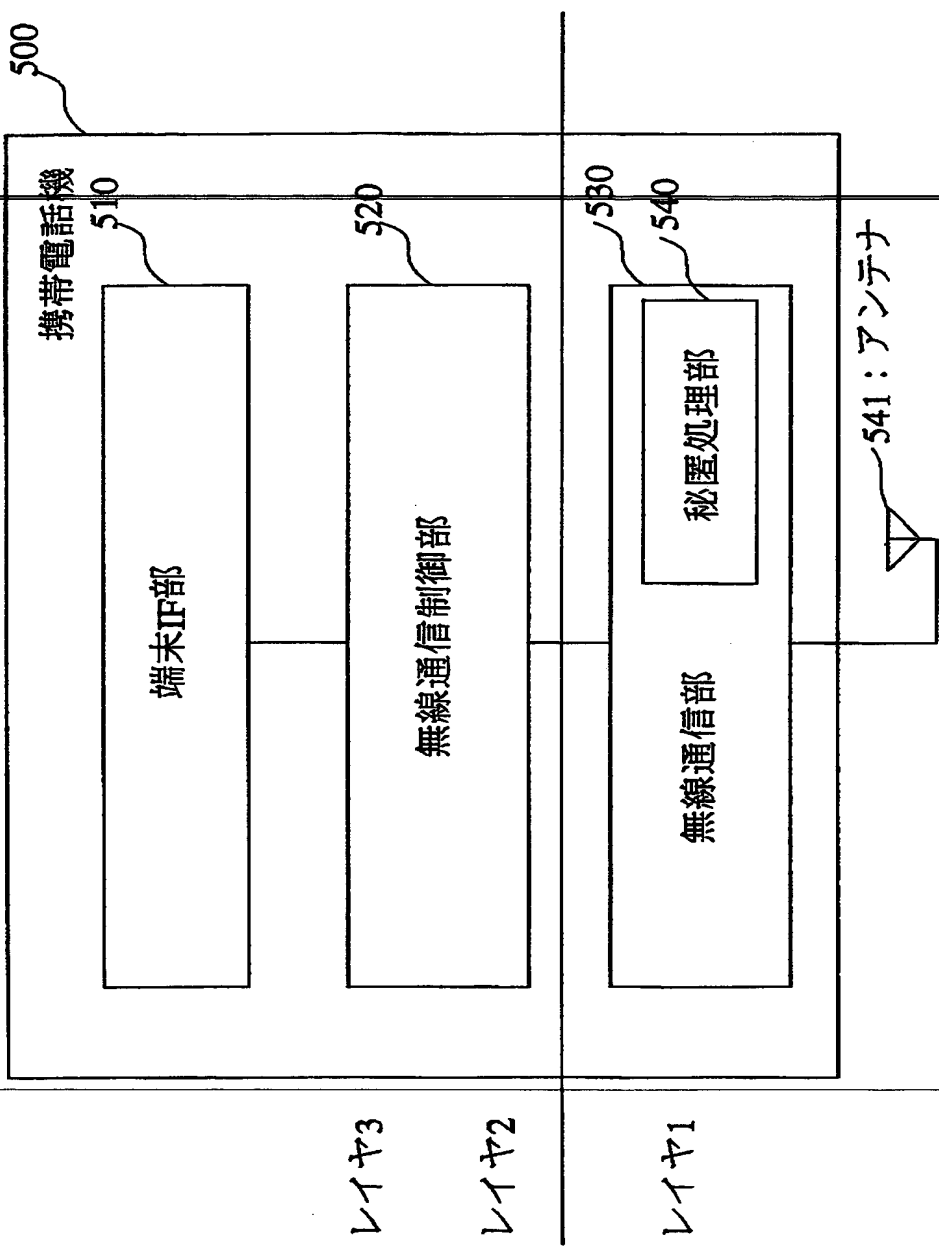
【図 1 2】



【図 1 3】



【図 1 4】



【書類名】 要約書

【要約】

【課題】 レイヤ 2 以上の上位レイヤにおいて秘匿処理及び完全性保証処理が行える無線端末 (MS) 1 0 0 を提供したい。

【解決手段】 端末 I F 部 1 0 と無線通信制御部 2 0 と無線通信部 3 0 との間に秘匿・完全性保証処理部 4 0 を設ける。秘匿・完全性保証処理部 4 0 は、端末 I F 部 1 0 と無線通信部 3 0 との間で音声データ等の透過データに対して秘匿処理のみを行う。秘匿・完全性保証処理部 4 0 は、無線通信制御部 2 0 との間で非透過データに対して秘匿処理又は／及び完全性保証処理を行う。秘匿・完全性保証処理部 4 0 は、無線通信部 3 0 から出力されたレイヤ 2 以上の上位階層のデータに対してデータの種別に応じて選択的に秘匿処理、完全性保証処理を行う。

【選択図】 図 9

出 願 人 履 歴 情 報

識別番号

[000006013]

1. 変更年月日	1990年 8月24日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目2番3号
氏 名	三菱電機株式会社

THIS PAGE BLANK (USPTO)